UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

BERNADINE GRIFFITH et al.,

Plaintiffs,

v.

TIKTOK, INC. et al.,

Defendants.

UNDER SEAL[1]

Case No. 5:23-cv-00964-SB-E

ORDER GRANTING DEFENDANTS' MOTION FOR SUMMARY JUDGMENT [DKT. NO. 266] AND DENYING AS MOOT MOTION FOR REVIEW OF DISCOVERY RULING [DKT. NO. 364]

Plaintiffs filed this case as a putative class challenging Defendants TikTok, Inc. and ByteDance, Inc.'s use of software to collect information about non-TikTok users when they visit third-party websites that have installed Defendants' software. Following denial of class certification, Defendants move for summary judgment on the claims of the three remaining individual plaintiffs—Bernadine Griffith, Patricia Shih, and Jacob Watters. Dkt. No. 266. The Court held a hearing on December 20, 2024. Because Plaintiffs have not produced evidence sufficient

[1] Because some of the briefing and exhibits filed in connection with the motion for summary judgment are under seal, the Court has preliminarily sealed this order. The Court expects to unseal the order unless the parties show a compelling reason not to. Within four business days after entry of this order, the parties shall meet and confer and file a joint statement as to whether any part of this opinion should remain sealed. If the parties do not agree that the order should be unsealed in its entirety, they shall propose specific redactions and explain the need for each redaction sought.

to raise genuine issues of material fact as to any of their claims, Defendants are entitled to summary judgment.[2]

I.

At the heart of this case are two software tools developed by Defendants[3] for use by third parties who wish to share information about visits to their websites with Defendants to improve targeted advertising. The Pixel, on which the parties principally focus, is a piece of code that can be embedded on webpages to send Defendants information about visits to the webpage. Joint Appendix of Facts (JAF) 1, Dkt. No. 269-2.[4] The Pixel is triggered by "events"—designated user actions on a website that has the Pixel installed. These can include standard events such as adding payment information, adding items to a shopping cart, completing registration, searching, and completing payment, or custom events that the website owners can define for themselves. Joint Appendix of Evidence (JAE) 30 ¶ 34.[5] Regardless of which events the website owner selects when configuring the Pixel, the Pixel by default always collects data through the "PageView" event, which is triggered when a visitor loads a webpage with the Pixel installed. *Id.* ¶ 35. For all

[2] The parties have submitted an extensive summary judgment record, and it is their responsibility to cite the relevant portions of the record to support their arguments, as a court reasonably cannot be expected to mine the record for them. Furthermore, Plaintiffs confirmed at the hearing that they did not omit anything from their papers that should be taken into account. Therefore, the Court considers only the cited record and finds that any argument is forfeited to the extent that it relies on an uncited portion.

[3] As with their prior motions, the parties largely conflate Defendants, and the Court does not distinguish between them for purposes of this order.

[4] The Court cites to the unredacted versions of the summary judgment materials filed under seal. Unless otherwise indicated, citations to the JAF are to undisputed facts, to the undisputed portions of partially disputed facts, or to the portions of disputed facts that do not appear to be genuinely in dispute based on the stated dispute. *See* Dkt. No. 42 at 6 ("If a party disputes a fact in bad faith by offering evidence that does not contradict the proffered fact *or* by failing to provide a specific citation to the supporting evidence, the Court will deem the fact undisputed for purposes of the motion.").

[5] The unredacted JAE is filed in six parts at Dkt. Nos. 269-43 through 269-48. The Court cites to the JAE by exhibit number and page or paragraph.

events, the Pixel collects seven categories of data: (1) timestamp, (2) IP address, (3) user agent, (4) cookies, (5) URL, (6) event information, and (7) content information. JAF 22.

The second tool, Events API (EAPI), is a server-to-server tool that sends similar information directly from the website owner's server to Defendants. JAF 2. Both the Pixel and EAPI collect and send information about website visitors to Defendants without distinguishing between TikTok users and non-users; Defendants then attempt to match the data to their records of TikTok users. JAF 5. Defendants use probabilistic matching to connect data acquired through the Pixel and EAPI to TikTok users through the IP address and user agent data. JAF 23. Defendants discard the data they are unable to match to TikTok users after 14 days, although the parties dispute whether the unmatched data has value to Defendants before it is deleted.

Plaintiffs are three individuals who have never used TikTok and who object to Defendants' collection of their browsing information through the Pixel and EAPI. Their claims therefore depend on the information Defendants have obtained from their online activity. Identifying that information, however, is challenging for three reasons.

First, the scope of Defendants' collection imposes practical problems for identifying Plaintiffs' data. The volume of information obtained by Defendants is massive, and its preservation is expensive. As the Court recounted in more detail in its October 10, 2024 order denying Plaintiffs' motion for discovery sanctions, Dkt. No. 283, Plaintiffs sought early in the litigation to require Defendants to suspend their practice of deleting unmatched data after 14 days, but the magistrate judge denied their request, instead ordering production of a one-day sample. Plaintiffs later rejected a proposal for them to pay the cost of maintaining the data they wanted preserved, which would be more than $2.5 million. The parties therefore proceeded on a sampling basis, and the summary judgment record is derived largely from the data collected by Defendants on two days: March 28 and May 21, 2024. That data included information Plaintiffs were able to link to Griffith and Watters, although no data was collected from Shih on the two days in the sample. JAE 58 ¶ 5. Plaintiffs also compared their browsing histories with the more than 600,000 websites in the two-day sample to identify times on other days that they visited webpages from the sample, suggesting that Defendants would have collected data from all three Plaintiffs—*if* the websites used the Pixel or EAPI on the dates of Plaintiffs' visits. *Id*. Thus, Plaintiffs rely largely (and in Shih's

case, exclusively) on inference rather than direct evidence of data collected by Defendants.

Second, Plaintiffs have litigated this case as a putative class action, focusing on Defendants' practices as a whole rather than on Plaintiffs' browsing activity. The resources expended on this case are vastly disproportionate to the value of Plaintiffs' individual claims. *See, e.g.*, Dkt. No. 283 at 4 (noting that even after denial of class certification, Plaintiffs obtained nearly 300 pages of expert reports despite their experts' approximation of each Plaintiff's damages as $93 under a restitution model and $10.24 on an unjust enrichment theory). As a result, much of the evidence before the Court involves Defendants' collection of data from other internet users, which is at most tangentially relevant to Plaintiffs' claims.

Third, the parties' approach to the summary judgment motion has not made the Court's review of the facts easy. The parties have filed approximately 19,000 pages of exhibits. The JAF does not directly identify the data Defendants obtained from Plaintiffs. Instead, the parties assert competing and sweeping disputed statements like "No sensitive personal information of Plaintiffs was disclosed to or collected by Defendants through the Pixel" and "Defendants' . . . sample data confirm that Defendants collected personally identifying data on Griffith." JAF 6, 26. The parties' statements in the JAF largely cite to their competing expert reports, which make representations—some highly generalized—about the underlying data. *See, e.g.*, JAE 58 ¶ 34 ("I found that tens of thousands of URLs from each plaintiff overlapped with the list of unique website domains of the websites that used the Pixel and/or EAPI (at least as of March 28, 2024 and May 21, 2024).").[6]

[6] The parties have filed more than 100 pages of objections. Dkt. No. 305-1. To the extent the Court relies on evidence to which an evidentiary objection was raised, the Court overrules the objection, having found the contents of the evidence could be admitted at trial. *See, e.g.*, *Sandoval v. County of San Diego*, 985 F.3d 657, 666 (9th Cir. 2021) ("If the contents of a document can be presented in a form that would be admissible at trial—for example, through live testimony by the author of the document—the mere fact that the document itself might be excludable hearsay provides no basis for refusing to consider it on summary judgment."). To the extent the Court does not rely on evidence objected to by the parties, the objections are overruled as moot.

The difficulty that arises from the parties' use of experts to indirectly establish the relevant facts is compounded by errors in the opinions of Plaintiffs' principal expert, Dr. Zubair Shafiq. In its October 22, 2024 order denying reconsideration of its denial of class certification, the Court identified numerous serious problems with Dr. Shafiq's September 20 report. Dkt. No. 337 at 3–4. Indeed, Plaintiffs acknowledged those problems, disclaiming reliance on the September 20 report and instead seeking to rely on a new October 11 rebuttal report by Dr. Shafiq. In connection with the summary judgment motion, Plaintiffs relied heavily on Dr. Shafiq's September 20 report, filed at JAE 57, as well as a September 30 report containing many similar opinions, filed at JAE 58. Two weeks after the motion was filed, Plaintiffs filed a "notice of correction" seeking to excise numerous statements in the joint brief and JAF that were based on erroneous analysis in Dr. Shafiq's September 20 and 30 reports. Dkt. No. 309. Plaintiffs reference Dr. Shafiq's revised opinions in the October 11 report, but that report is not properly before the Court as part of the summary judgment record. The Court is therefore left to attempt to discern the relevant underlying facts from the portions of the expert reports that have not been withdrawn.

As modified by their notice of correction, it appears that Plaintiffs have identified several dozen events associated with Griffith in the two-day sample and one event associated with Watters. Dr. Shafiq identifies only one of these as potentially sensitive: a URL for a page confirming Griffith's purchase of two pillowcases. JAE 58 ¶ 32. The examples of Watters's sensitive searches on which Plaintiffs relied in the joint brief have all been withdrawn.

Apart from the two-day sample, Plaintiffs in their briefing identify 23 URLs from Plaintiffs' browsing histories that correspond to websites that—as of the dates in the two-day sample—had the Pixel or EAPI installed. Dkt. No. 332 at 14–15 (citing JAE 57 ¶ 65). Plaintiffs do not identify when they visited these URLs, and there is no direct evidence of what information, if any, Defendants received from Plaintiffs' visits. All three Plaintiffs configured their browser settings or used software to block cookies and, in the case of Shih, to obscure her IP address. JAF 18–21.

Following two rounds of pleading challenges and voluntary dismissals by other plaintiffs, the operative Second Amended Complaint (SAC) alleges claims for (1) violation of the California Invasion of Privacy Act (CIPA), (2) statutory larceny under §§ 484 and 496 of the California Penal Code, (3) conversion, (4) invasion of privacy under the California Constitution, (5) intrusion on

seclusion, and (6) violation of the Electronic Communication Privacy Act (ECPA). Dkt. No. 137. The Court denied Plaintiffs' motions for class certification and for reconsideration of the denial. Dkt. Nos. 242, 337. Defendants now move for summary judgment on all claims. Dkt. No. 266.

II.

Summary judgment is appropriate where the record, taken in the light most favorable to the opposing party, shows "that there is no genuine dispute as to any material fact and the movant is entitled to judgment as a matter of law." Fed. R. Civ. P. 56(a); *see also Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 247–48 (1986). "The evidence of the non-movant is to be believed, and all justifiable inferences are to be drawn in his favor." *Anderson*, 477 U.S. at 255. The moving party has the initial burden of establishing that there are no disputed material facts. *Id*. at 256. "If a party fails to properly support an assertion of fact or fails to properly address another party's assertion of fact . . . the court may . . . consider the fact undisputed." Fed. R. Civ. P. 56(e)(2). Furthermore, "Rule 56[(a)] mandates the entry of summary judgment . . . against a party who fails to make a showing sufficient to establish the existence of an element essential to that party's case, and on which that party will bear the burden of proof at trial." *Celotex Corp. v. Catrett*, 477 U.S. 317, 322 (1986). Where the court does not grant a party's requested relief, it may still grant partial relief on distinct issues or facts. *See* Fed. R. Civ. P. 56(g).

III.

Before turning to the claim-specific arguments raised in the motion for summary judgment, the Court first addresses a fundamental dispute about the evidence that may be properly considered in support of Plaintiffs' claims. In their reply, Defendants argue that Plaintiffs had refused discovery into their browsing history—except for their browsing on the websites identified in the complaint—and that they should not now be able to rely on their entire browsing history. Dkt. No. 350 at 1–2. The Court ordered supplemental briefing on that issue. Dkt. No. 374.

It is undisputed that Defendants requested Plaintiffs' entire browsing history and, more narrowly, their browsing history for all visits to websites that used the Pixel. Dkt. No. 376 at 2–4. Plaintiffs declined to produce their full browsing history, asserting that visits to sites that did not use the Pixel were irrelevant, and they were initially unable to produce their browsing history for websites that used

the Pixel because they did not know which websites used it. Dkt. No. 376-1 ¶¶ 3–7. After Defendants produced the two-day sample in August 2024, Plaintiffs compared the websites in the sample to their browsing history and produced to Defendants on September 20 and 30 a list of URLs they had visited that overlapped with domains in the sample data. *Id.* ¶ 8. This list of URLs, which spans more than 8,000 pages, is at JAE 67. It contains no timestamps, metadata, or other information about when Plaintiffs visited the URLs. Plaintiffs later produced the actual data from their browsing histories to Defendants on October 11, but it is not part of the summary judgment record (or otherwise before the Court). Dkt. No. 376 at 4; Dkt. No. 376-1 ¶ 10.

On this record, particularly considering the delays in Defendants' production of their own discovery, the Court will not exclude as untimely the evidence of URLs visited by Plaintiffs in JAE 67. However, that list of URLs has little meaning in the absence of information about when Plaintiffs visited the URLs and whether the sites had the Pixel or EAPI installed at the time of the visits—information Plaintiffs have not included in the summary judgment record. Dr. Shafiq's reports analyzing the browsing history do not address the timing of the visits. *See* JAE 57 ¶ 65 (stating that Dr. Shafiq found URLs visited by Plaintiffs that overlapped with the websites in the two-day sample without addressing when Plaintiffs visited the URLs or whether the URLs used the Pixel or EAPI at the time); JAE 58 ¶ 34 (same). Nor does Dr. Shafiq address when the websites Plaintiffs visited began using the Pixel and EAPI or whether they continue to use them. *See, e.g.*, JAE 58 ¶ 6 (explaining that JAE 67 represents "Plaintiffs' browsing histories of websites that use Pixel and/or EAPI *as of March 28 or May 21*.") (emphasis added).[7]

Without information about when Plaintiffs visited the identified websites and whether the websites had the Pixel or EAPI installed at the time, Plaintiffs are unable to cite to any nonspeculative evidence in the summary judgment record that Defendants obtained any information from any of Plaintiffs' visits to the URLs.[8]

---

[7] While Plaintiffs have repeatedly contended that Defendants withheld or delayed discovery, they acknowledged at the hearing that they were able to obtain information about the websites' use of the Pixel directly from the website owners through subpoenas. It appears that Plaintiffs did not rely on the information obtained through those subpoenas in their summary judgment papers.

[8] Moreover, given that each Plaintiff employed settings or tools to block the transmission of information, JAF 18–21, it is not clear on this record what

For example, Plaintiffs cite no evidence that www.pinkblushmaternity.com had the Pixel or EAPI installed when Griffith browsed a maternity jumpsuit on that site, and no evidence that Defendants received any information about Griffith's visit to the site. Plaintiffs' browsing history, at least in the form presented on this motion, and Dr. Shafiq's discussion of that history do not therefore raise a fact issue as to any information collected from Plaintiffs by Defendants. Accordingly, the relevant evidence of information collected by Defendants is limited to the two-day sample. Because that data contains no evidence that Defendants collected any information—sensitive or otherwise—from Plaintiff Shih, Defendants are entitled to summary judgment on her claims.[9]

IV.

Defendants seek summary judgment on four grounds, arguing that (1) Plaintiffs expressly and impliedly consented to the collection of their information, (2) there is no evidence that Plaintiffs' private information was disclosed to Defendants, (3) the Pixel and EAPI did not intercept the contents of

---

information Defendants would have received even if the URLs did employ the Pixel or EAPI.

[9] Plaintiffs' arguments focus on the two-day sample and Plaintiffs' browsing history. Dr. Shafiq, however, also opined on the statistical likelihood that Defendants collect sensitive data from average non-TikTok users, *e.g.*, JAE 58 ¶ 10 ("[T]he probability that TikTok collected one or more sensitive URLs from an average non-TikTok user is 43% for one day, 98% for one week, and 100% for a month or more."), although he subsequently revised those probabilities downward in his October 11 rebuttal report, which is not part of the summary judgment record, Dkt. No. 297-2 ¶ 56. In denying class certification, the Court noted multiple unsupported assumptions in Dr. Shafiq's projections about average internet users. Dkt. No. 242 at 14. Indeed, the fact that Defendants collected no information whatsoever from Plaintiff Shih in the two days sampled suggests either that she is not an average non-user of TikTok or that Dr. Shafiq's assumptions and conclusions are erroneous, further supporting the Court's previous finding that Plaintiffs had not established typicality for purposes of class certification. In any event, Plaintiffs have not argued or shown in connection with the summary judgment motion that they are average non-users of TikTok, so it is unnecessary to determine whether Dr. Shafiq's statistical projections about the likelihood of Defendants collecting information from average non-users could by themselves create a genuine issue of material fact as to collection from Plaintiffs.

Plaintiffs' communications, and (4) Plaintiffs lack a property interest in the data collected by Defendants.

A.

If Defendants can show that Plaintiffs consented to Defendants' collection of their data through the Pixel and EAPI, Plaintiffs' claims undisputedly fail because lack of consent is an element of their CIPA claims and a defense to their other claims. *See Calhoun v. Google LLC*, 526 F. Supp. 3d 605, 619 (N.D. Cal. 2021) (collecting cases showing that consent defeats claims for common-law privacy violations, theft, and wiretapping and eavesdropping under the Wiretap Act and CIPA).

Consent can be express or implied, but it must be actual. *Calhoun v. Google, LLC*, 113 F.4th 1141, 1147 (9th Cir. 2024). Defendants invoke both forms of consent, arguing that (1) Plaintiffs expressly agreed to the terms of service on the websites for which they created accounts, and those terms disclosed that their information would be shared with third parties; and (2) Plaintiffs impliedly consented to the collection of their data when they continued using websites after filing this lawsuit, knowing that the websites used the Pixel and transmitted data to Defendants. These arguments are limited to the websites identified in the pleadings; Defendants do not attempt to show either express or implied consent as to any of the other hundreds of thousands of websites that have employed the Pixel or EAPI, including, for example, the website on which Griffith purchased pillowcases during the two-day sample.

1.

"For consent to be actual, the disclosures must explicitly notify users of the conduct at issue," and "consent is only effective if the person alleging harm consented to the particular conduct, or to substantially the same conduct and if the alleged tortfeasor did not exceed the scope of that consent." *Id*. (cleaned up). If a user could have plausibly understood a disclosure as *not* disclosing the particular conduct by the defendant, the disclosure is insufficient to establish consent. *Id*. In determining the scope of consent, the court must consider what a reasonable user would understand without "attributing to that user the skill of an experienced business lawyer or someone who is able to easily ferret through a labyrinth of legal jargon to understand what he or she is consenting to." *Id*. at 1151.

Defendants identify various disclosures from the privacy policies of Rite Aid, Hulu, Etsy, and Upwork to which they contend Plaintiffs agreed. JAF 47–76. These policies disclosed that the websites would collect certain information and share it with certain third parties. Rite Aid disclosed that information would be shared with "third parties who perform services on our behalf" and with "advertising partners." JAF 48–49. Hulu at various times disclosed that "third party Internet advertising companies" would collect users' information and that information might be shared with third parties, including business partners, social networking services, advertisers, and other companies. JAF 52–53. Etsy disclosed that information would be shared with "certain third-party service providers." JAF 58, 61. Upwork disclosed that "third party service providers" and "network advertisers, ad agencies, analytics service providers[,] and other vendors" might have access to data obtained from users. JAE 65, 70, 76. It is undisputed that none of the privacy policies mentioned TikTok by name or expressly disclosed that data would be shared with Defendants. JAF 84. It is also undisputed that TikTok does not describe itself as an advertiser. JAF 85. And there is no suggestion that Defendants themselves made any relevant disclosure to Plaintiffs about their collection of Plaintiffs' data.

Defendants have not shown as a matter of law that Plaintiffs actually consented to the use of the Pixel and EAPI to send their data to Defendants. Even setting aside Plaintiffs' objections and arguments about whether they agreed to the websites' terms, a reasonable user reviewing those terms would not necessarily understand that Defendants were among the advertisers or business partners with whom the websites would share visitors' information. Moreover, Plaintiffs have identified widespread heightened privacy concerns specific to TikTok due to its size, foreign ownership, and perceived activities. *See, e.g.*, Dkt. No. 137 ¶¶ 29–37 (alleging public concerns about TikTok and that "Defendants' mass collection of private data from ordinary Americans poses a unique national security threat due to the fact that Defendants are effectively controlled by the Chinese government"). Especially in light of those concerns, it is not clear that reasonable users of the websites at issue would understand that their information would be shared with Defendants based on vague disclosures about collection by advertising partners or service providers. On this record, the Court cannot conclude as a matter of law that Plaintiffs actually consented to Defendants' acquisition of their browsing data.[10]

[10] Defendants' cited cases are distinguishable. *Smith v. Facebook, Inc.* involved Facebook's tracking of its own users' activity, which it disclosed in the terms of agreement when its users signed up for Facebook accounts. 262 F. Supp. 3d 943,

2.

Defendants also argue that Plaintiffs impliedly consented to the collection of their data through their course of conduct when, after filing this lawsuit, they continued to visit the sites they knew were using the Pixel and EAPI. If successful, this argument would provide a partial defense, limited to collection of data from the websites identified in the complaint after each Plaintiff joined the litigation.

It is undisputed that Griffith continued to visit the Hulu, Etsy, and Build-A-Bear websites after filing this action, that Watters visited the Etsy website after joining the action, and that both Plaintiffs knew that information about those visits might be shared with Defendants. JAF 77, 79. Each Plaintiff also declared that he or she did not consent to Defendants' collection of his or her data, and Watters testified that he would not knowingly use a website with the Pixel installed unless he had no other choice. JAF 86, 88.

Defendants rely principally on out-of-circuit authority explaining that in the ECPA context, implied consent may be "inferred from surrounding circumstances indicating that the party knowingly agreed to the surveillance." *Berry v. Funk*, 146 F.3d 1003, 1011 (D.C. Cir. 1998) (cleaned up). Defendants also invoke the California Supreme Court's explanation that "the plaintiff in an invasion of privacy case must have conducted himself or herself in a manner consistent with an actual expectation of privacy, i.e., he or she must not have manifested by his or her conduct a voluntary consent to the invasive actions of defendant." *Hill v. Nat'l Collegiate Athletic Assn.*, 7 Cal. 4th 1, 26 (1994).

Neither *Berry* nor *Hill* involved an invocation of implied consent based on conduct after the plaintiff had filed a lawsuit challenging the defendant's invasion of privacy.[11] While it may be reasonable to infer that someone who learns of

---

953 (N.D. Cal. 2017). In *In re Yahoo Mail Litigation*, Yahoo expressly disclosed that it scanned and analyzed all incoming and outgoing emails—the conduct challenged in that case. 7 F. Supp. 3d 1016, 1029 (N.D. Cal. 2014). Here, in contrast, there was no disclosure that Defendants would have any involvement in Plaintiffs' browsing activity, let alone a disclosure of the specific conduct challenged.

[11] The analysis in *Hill* tends to suggest a different argument—that Plaintiffs cannot claim a reasonable expectation of privacy for purposes of their claims for intrusion on seclusion and invasion of privacy because they knew their activity was not

surveillance and continues to subject herself to the surveillance without taking any other action has agreed to the surveillance, it is not obvious that the same inference may be drawn when the person files or joins a lawsuit claiming that the surveillance is unlawful. Indeed, Defendants do not explain why the filing of a lawsuit challenging TikTok's practice is not part of the "surrounding circumstances" from which the factfinder should determine whether Plaintiffs "knowingly agreed to the surveillance." *Berry*, 146 F.3d at 1011. They also acknowledged at the hearing that they had not identified any cases finding implied consent based on similar post-litigation conduct. In fact, courts have rejected arguments that litigants must stop using a defendant's products to avoid being found to have consented to the conduct they are challenging in the lawsuit. *See Rodriguez v. Google LLC*, No. 20-CV-04688, 2024 WL 38302, at *5 (N.D. Cal. Jan. 3, 2024) (noting that "Google's argument places an impossible burden on Plaintiffs that would preclude injunctive relief altogether: they must stop using the many apps on their phones to avoid consenting to the wrongful conduct, unfairly undercutting standing to seek injunctive relief"); *In re Yahoo Mail Litig.*, 308 F.R.D. 577, 589 (N.D. Cal. 2015) (rejecting argument that plaintiffs needed to stop exchanging emails with Yahoo users to avoid consenting to Yahoo's conduct because it "would put Plaintiffs in a catch–22 that would essentially preclude injunctive relief altogether").

On this record, a reasonable jury could conclude that Plaintiffs did not knowingly agree to Defendants' collection of their data when they continued to use third-party websites after filing a lawsuit alleging that Defendants' collection of their data from those websites was unlawful. Defendants therefore have not shown that they are entitled to summary judgment based on consent.

B.

Defendants next argue that Plaintiffs' claims for invasion of privacy, intrusion on seclusion, and violation of CIPA § 632[12] fail because there is no evidence that any private information about Plaintiffs was disclosed to Defendants.

---

private. Defendants raised this argument for the first time at the hearing. The Court declines to reach it because their citation to *Hill* in their arguments about consent did not give Plaintiffs fair notice.

[12] Count 1 of the SAC alleges violations of two separate provisions of CIPA: the prohibition on wiretapping in Cal. Penal Code § 631 and the prohibition on recording in Cal. Penal Code § 632. The parties address § 632 together with the

The first two claims, often considered together, require the existence of a reasonable expectation of privacy and a highly offensive intrusion. *In re Facebook, Inc. Internet Tracking Litig.* (*Facebook Tracking*), 956 F.3d 589, 601 (9th Cir. 2020) (citing *Hernandez v. Hillsides, Inc.*, 47 Cal. 4th 272, 287 (2009)). "The existence of a reasonable expectation of privacy, given the circumstances of each case, is a mixed question of law and fact." *See id.* (citing *Hill*, 7 Cal. 4th at 40).

Section 632, which forms the basis of the third claim, prohibits the recording of "confidential" communications. Cal. Penal Code § 632(a). A conversation is confidential under § 632 "if a party to that conversation has an objectively reasonable expectation that the conversation is not being overheard or recorded." *Flanagan v. Flanagan*, 27 Cal. 4th 766, 777 (2002). Courts in California "have developed a presumption that Internet communications do not reasonably give rise to that expectation." *Revitch v. New Moosejaw, LLC*, No. 18-CV-06827, 2019 WL 5485330, at *3 (N.D. Cal. Oct. 23, 2019) (collecting cases). To overcome that presumption, a plaintiff must show "that there is something unique about [their] particular internet communications which justify departing from the presumption." *In re Meta Pixel Healthcare Litig.*, 647 F. Supp. 3d 778, 799 (N.D. Cal. 2022) (finding presumption overcome, for purposes of preliminary injunction, based on context of communications with medical providers). Courts have recognized similarities in the analysis of whether a reasonable expectation of privacy exists for purposes of California privacy claims and whether a conversation is confidential under CIPA § 632, *id*. at 800 n.12, and both sides address these claims together.[13]

The parties dispute whether information must be both sensitive and personally identifiable to create a reasonable expectation of privacy.[14] Regardless,

---

claims for invasion of privacy and intrusion on seclusion and address § 631 together with the federal wiretap prohibitions in the ECPA, discussed below.

[13] Because the parties treat the standards applicable to these claims as if they were the same, this Court does not consider whether they are identical in all respects. *See* Dkt. No. 59 at 10–11 (noting that this question is not entirely clear).

[14] Plaintiffs rely on a statement in a district court decision addressing the ECPA that "information need not be personally identifying to be private." *In re Google Referrer Header Priv. Litig.*, 465 F. Supp. 3d 999, 1009–10 (N.D. Cal. 2020). This language, which is not controlling authority, did not address the reasonable expectation of privacy required for the California privacy claims at issue here.

Plaintiffs have failed to produce evidence that Defendants collected sensitive information from them. *Facebook Tracking* is instructive. In that case, the plaintiffs alleged that Facebook tracked its users' internet browsing even when they logged out of Facebook, allegedly in tension with its representations that logged-out data would not be collected. This allowed Facebook to "amass a great degree of personalized information" including "an individual's likes, dislikes, interests, and habits over a significant amount of time," all of which could be tied to the Facebook user's identity. *Id*. at 599. In addressing the nature of the data collected, the court emphasized that "Facebook obtained a comprehensive browsing history of an individual, no matter how sensitive the websites visited." *Id*. at 603. Moreover, because Facebook also had access to users' profiles, which "could include a user's employment history and political and religious affiliations," its tracking of the users' browsing activity allowed it to "gain[] a cradle-to-grave profile without users' consent." *Id*. at 599. Under these circumstances, the Ninth Circuit found that the plaintiffs had plausibly alleged that Facebook violated their reasonable expectation of privacy.

The facts here differ greatly from those in *Facebook Tracking*. First, Plaintiffs are not TikTok users, so Defendants do not have access to profile information for them similar to that possessed by Facebook. While Plaintiffs' expert was able to identify data obtained from Griffith and Watters in the two-day sample by correlating it to information he obtained from Plaintiffs' computers, there is no evidence that Defendants would have been able to identify the data as belonging to Plaintiffs without that additional information.[15] The Pixel and EAPI are also installed on a relatively small percentage of websites—still a large number in absolute terms, but not enough to capture Plaintiffs' "comprehensive browsing history." And Plaintiffs have not identified any particularly sensitive information Defendants collected from them.

In arguing to the contrary, Plaintiffs rely on (1) examples from the two-day sample and (2) examples from Plaintiffs' browsing history. Dkt. No. 332 at 12–15. But every example of sensitive information they identified from the two-day sample was based on errors in Dr. Shafiq's analysis, which Plaintiffs later withdrew. Dkt. No. 309 at 2 (notice of correction deleting references to "URLs that a reasonable juror could deem sensitive"). Plaintiffs also withdrew the

[15] At the hearing, Plaintiffs' counsel, when specifically asked, was unable to identify any record evidence showing that Dr. Shafiq could have identified Plaintiffs' information from the two-day sample without access to their computers.

paragraph of Dr. Shafiq's report stating that the two-day sample contained potentially sensitive data from Plaintiffs, as well as 21 of the 22 specific examples he provided of websites Griffith and Watters had purportedly visited. *Id*. at 3 (deleting references to ¶¶ 9, 11–31, and 33 of Dr. Shafiq's report at JAE 58). And as discussed above, Plaintiffs' browsing history does not demonstrate collection of information by Defendants because Plaintiffs have not identified evidence of when they visited the sites or whether the Pixel or EAPI was active at the time.

Thus, Plaintiffs' briefing fails to identify any sensitive information collected from them. Following their retractions, Plaintiffs do not identify any data from the two-day sample that contains sensitive information about any of them. From what remains of Dr. Shafiq's report, it appears that the only relevant website browsing history identified from the two-day sample is Griffith's visit to Southshore Fine Linens, where she bought two pillowcases. JAE 58 ¶ 32. Plaintiffs do not even mention this history in their briefing, much less argue that Griffith's purchase of pillowcases was entitled to a reasonable expectation of privacy.

Lacking the evidence to prove their claims, Plaintiffs invoke their motion for discovery sanctions (which was pending at the time of the briefing), contending that Defendants spoliated evidence by deleting the non-user data they collected after 14 days, pursuant to their data retention policy. But the Court struck that motion as untimely and explained that it also failed because the magistrate judge had rejected Plaintiffs' request to order retention of the data, and the parties had proceeded on a sampling basis instead. Dkt. No. 283. Addressing Plaintiffs' fairness argument, the Court explained:

> Regardless of Plaintiffs' motion, the Court does not intend to permit Defendants "to treat the two-day sample produced as if it constituted the universe of non-TikTok user data that they collected," as Plaintiffs fear, Dkt. No. 264-1 at 27, nor does the Court understand Defendants to be making any such argument. The Court and all parties recognize that the samples produced by Defendants are just that—samples. Neither side has argued that the samples are nonrepresentative. Thus, it is reasonable to infer that the deleted data was similar to the data in the samples, and the Court does not understand Defendants to argue otherwise. On the other hand, Plaintiffs have not shown any basis for the Court to infer that the deleted data contained evidence necessary to support their claims that is materially different from the data in the sample, and the Court will not allow Plaintiffs to circumvent their burden by effectively requesting an assumption that the deleted data

> would supply missing elements (to the extent that elements are missing, which the Court does not now decide) as a sanction for Defendants' nonpreservation of data that Judge Eick did not order them to preserve.

Id. at 4–5.

Applying that approach here, if Plaintiffs had identified only a small volume of sensitive information collected from them in the two-day sample, the Court would have permitted the reasonable inference that similar information was likely collected on other days when they visited the relevant websites and TikTok was gathering data from those sites, such that Defendants would not be entitled to summary judgment based only on the size of the sample. But Plaintiffs have not identified any sensitive information collected from Griffith or Watters (or any information at all from Shih) in the two-day sample. There is thus no reasonable basis to assume that Defendants collected sensitive information from them on other days—i.e., that the sample is nonrepresentative.

In short, Plaintiffs have not produced evidence of any sensitive information Defendants collected from them. Nor have Plaintiffs shown that Defendants collected vast quantities of identifiable data from them that would allow Defendants to create the type of "cradle-to-grave profiles" at issue in *Facebook Tracking*—much less that Defendants actually created such profiles. *Cf. Facebook Tracking*, 956 F.3d at 604 ("[V]iewing the allegations in the light most favorable to Plaintiffs, as we must at this stage, the allegations that Facebook allegedly compiled highly personalized profiles from sensitive browsing histories and habits prevent us from concluding that the Plaintiffs have no reasonable expectation of privacy."). To be sure, Plaintiffs *alleged* such collection, and the Court found their allegations sufficient to survive a pleading challenge. Dkt. No. 59 at 6–10. But plausible allegations are not enough at the summary judgment stage.[16] On this

[16] Rule 56 permits a party to request that the Court defer ruling on a summary judgment motion because the party needs more time to present facts necessary to justify its opposition. Fed. R. Civ. P. 56(d). Although the parties were still in the process of exchanging discovery during the summary judgment briefing, and additional evidence was developed after the motion was filed (including Dr. Shafiq's revisions to his opinions), Plaintiffs did not request that the Court defer considering the motion under Rule 56(d). *See* Dkt. No. 362 at 5:7–11 (Plaintiffs' admission to magistrate judge that they did not request additional time under Rule 56(d)). Nor did they request additional time at the hearing—or argue that they had

record, no reasonable factfinder could determine that Plaintiffs have shown a reasonable expectation of privacy in any information Defendants collected from them. Defendants are therefore entitled to summary judgment on Plaintiffs' claims for invasion of privacy, intrusion on seclusion, and violation of CIPA § 632.

C.

Defendants next argue that Plaintiffs' wiretapping claims under the ECPA and § 631 of CIPA fail because (1) there is no evidence that Defendants collected the "contents" of any of Plaintiffs' communications, (2) the Pixel and EAPI do not intercept communications within the meaning of the statutes, and (3) any interception was done by the third-party websites rather than Defendants.

It is undisputed that Plaintiffs' claims under both the federal and state wiretapping statutes require them to show that Defendants intercepted the "contents" of a communication. The Ninth Circuit has explained that under the ECPA, "the term 'contents' refers to the intended message conveyed by the communication, and does not include record information regarding the characteristics of the message that is generated in the course of the communication." *In re Zynga Priv. Litig.*, 750 F.3d 1098, 1106 (9th Cir. 2014). "Under some circumstances, a user's request to a search engine for specific information could constitute a communication such that divulging a URL containing that search term to a third party could amount to disclosure of the contents of a communication," but a URL that merely contains "basic identification and address information" does not constitute contents of a communication. *Id*. at 1108–09. The analysis is the same for a CIPA § 631

---

been unable to produce the evidence they needed to survive summary judgment—instead affirming that nothing had been omitted from their papers. Having declined to seek relief under Rule 56(d), it is too late for Plaintiffs now to request another opportunity to fill the gaps in the summary judgment record. *Cf*. Dkt. No. 337 at 5 (rejecting argument that Plaintiffs should be allowed to file a new class certification motion because of Defendants' discovery delays) ("Had Plaintiffs informed the Court in advance of the class certification motion deadline that they still had not received the data necessary to file their motion, the Court might have allowed additional time. But Plaintiffs made no such request. Instead, they filed their class certification motion on June 21, claiming that they had satisfied their burden under Rule 23.").

interception claim. *Hammerling v. Google LLC*, 615 F. Supp. 3d 1069, 1092 (N.D. Cal. 2022).

In their brief, Plaintiffs identify five URLs that they contend are contents of their communications that were intercepted by Defendants. Dkt. No. 332 at 22–23. Two of those reflect activity erroneously attributed to Watters that Plaintiffs have withdrawn, and the other three are taken from Plaintiffs' browsing history, which does not support Plaintiffs' claims because—as already explained—there is no evidence that Defendants obtained information from Plaintiffs' visits to those websites. Thus, Plaintiffs have not identified any URLs intercepted by Defendants that constitute contents of a communication. *Cf. Brown v. Google LLC*, 685 F. Supp. 3d 909, 936 (N.D. Cal. 2023) (denying summary judgment on wiretap claim where intercepted URL disclosed "that the user was searching for updates on Russia's war against Ukraine on the Washington Post's 'World' section."). Plaintiffs also reference Dr. Shafiq's description of two categories of data uniformly collected—Event Information and Content Information—but cite no legal authority suggesting that this information constitutes "contents" of a communication for purposes of CIPA and the ECPA. Nor do they identify any specific Event Information or Content Information collected from any Plaintiff to show that it rises to the level of protected "contents." Accordingly, because Plaintiffs produce no evidence of any contents of a communication that Defendants obtained from them, Defendants are entitled to summary judgment on the CIPA and ECPA claims.

Even if Plaintiffs could identify qualifying contents of their communications obtained by Defendants, it appears that summary judgment would be appropriate—at least in part—on other grounds. While the record does not clearly explain exactly how the Pixel transmits data, it is undisputed that the EAPI shares information with Defendants only after it is received by advertisers. JAF 38. Plaintiffs emphasize that the information may be sent to Defendants within milliseconds, and even before a webpage has finished loading, but the Ninth Circuit has adopted a narrow definition of "interception" under the ECPA that focuses not only on timing but also on sequence. *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 878 (9th Cir. 2002) ("We therefore hold that for a website . . . to be 'intercepted' in violation of the Wiretap Act, it must be acquired *during transmission*, not while it is in electronic storage. This conclusion is consistent with the ordinary meaning of 'intercept,' which is 'to stop, seize, or interrupt *in progress or course before arrival*.'") (quoting Webster's Ninth New Collegiate Dictionary 630 (1985)) (footnote omitted, emphasis added). Because it does not appear that Defendants obtain any information "during transmission" (i.e. "before

arrival") from the EAPI, Plaintiffs cannot show an interception at least as to the EAPI.[17] That TikTok (and others) may refer to this transmission as occurring in real time is immaterial; it does not raise a fact issue as to whether the undisputed sequence of events falls within the narrow statutory definition of interception. Plaintiffs also failed to respond to Defendants' third argument—that any interception is the responsibility of the websites, not Defendants. Accordingly, it appears that Defendants are entitled to summary judgment on multiple grounds in addition to their failure to identify contents of their communications received by Defendants.

D.

Finally, Defendants seek summary judgment on Plaintiffs' claims for statutory larceny and conversion, arguing that Plaintiffs lack a property interest in the information collected by the Pixel and EAPI. The parties' dispute focuses on the legal question of whether and when a property interest exists in personal information.

The case law on this question is largely unhelpful. Most of the cases cited by both sides involve standing under California's Unfair Competition Law (UCL), which raises related but distinct issues. *See* Dkt. No. 59 at 19 n.7 (explaining that despite overlap in issues, Plaintiffs had plausibly alleged the existence of a property interest sufficient to support larceny and conversion claims but had not plausibly alleged economic loss for purposes of UCL standing). District courts in the Ninth Circuit have taken conflicting approaches to whether individuals possess a property interest in their personal information collected through online activity. *Compare Low v. LinkedIn Corp.*, 900 F. Supp. 2d 1010, 1030 (N.D. Cal. 2012) (dismissing conversion claim because "the weight of authority holds that a plaintiff's 'personal information' does not constitute property"), *with Calhoun*, 526 F. Supp. 3d at 635 (denying motion to dismiss statutory larceny claim and recognizing "growing trend across courts to recognize the lost property value of personal information") (cleaned up). The Ninth Circuit has not squarely addressed the issue but held in its standing analysis in *Facebook Tracking* that the plaintiffs had plausibly alleged an economic injury—including for their statutory larceny

[17] Plaintiffs rely on the Seventh Circuit's decision in *United States v. Szymuszkiewicz*, 622 F.3d 701, 705–06 (7th Cir. 2010), which, unlike the Ninth Circuit, appears to consider sequence unimportant if the transmission is sufficiently quick. This Court, of course, is bound to follow Ninth Circuit law.

claim—by alleging that their browsing histories had financial value and that Facebook had profited from selling their data to advertisers. 956 F.3d at 600–01.

Defendants also invoke controlling authority from other contexts holding more generally that the existence of a property right requires "exclusive possession or control," among other elements. *Kremen v. Cohen*, 337 F.3d 1024, 1030 (9th Cir. 2003). This would appear to preclude a finding that Plaintiffs had a property interest in the data created when they visited and interacted with websites, because they necessarily shared the underlying information for those interactions with the websites and internet service providers. But *Facebook Tracking* and the district court cases finding a property interest in browsing data do not address *Kremen* or related authority.

The Court does not approach the question of property interest on a blank slate. In their motion to dismiss the original complaint, Defendants invoked *Low* and briefly argued that Plaintiffs lacked a property interest in their data. The Court (1) noted that Judge Koh, the author of *Low*, had later reached a different conclusion in *Calhoun*; (2) observed that Defendants had conceded that personal information *can* be property; and (3) rejected Defendants' arguments that relied on facts outside the pleadings, concluding that Plaintiffs had alleged sufficient facts to survive a pleading challenge. Dkt. No. 59 at 14–16. Later, in denying class certification, the Court focused on the significance of the particular facts in determining the existence of a property interest. Dkt. No. 242 at 11 ("[W]hether class members have a cognizable property interest in the information sent to Defendants for purposes of their statutory larceny and conversion claims turns on the nature of that information and whether it carries financial value."). The Court observed that Plaintiffs had "produced expert testimony tending to support their contention that a market exists for the comprehensive browsing history of an active internet user," but had not "shown that a class member who briefly visits a few websites using the Pixel and shares no sensitive information has a marketable property interest in the data collected by the websites." *Id*.

It is unnecessary for purposes of this motion to reassess whether the prior orders recognizing a potential property interest in personal information collected by Defendants can be reconciled with the Ninth Circuit's requirement of exclusive possession or control as a prerequisite for a property right. Plaintiffs identify no cases finding a cognizable property interest based on facts similar to those in the summary judgment record. As discussed above, Plaintiffs have not shown that Defendants collected any sensitive information from them, nor is it even clear that Defendants obtained any personally identifiable information that Defendants

would be able to associate with Plaintiffs without being able to work backwards from information on Plaintiffs' computers, as Dr. Shafiq did. *Cf. Calhoun*, 526 F. Supp. 3d at 613 (allegations that Google identifies specific internet users and their devices and "engages in a controversial practice known as 'cookie synching' which further allows Google to associate cookies with specific individuals"); *Kis v. Cognism Inc.*, No. 22-CV-05322, 2024 WL 3924553, at *7 (N.D. Cal. Aug. 23, 2024) (finding UCL standing based on use of plaintiffs' names, likenesses, and photographs). Plaintiffs produce evidence that a few companies exist that pay users monthly to collect their browsing data, JAE 59 ¶¶ 103–08, but there is no specific evidence of any value associated with the small percentage of Griffith's and Watters's browsing histories that Defendants collected. Nor is there any suggestion that Plaintiffs' ability to monetize their own browsing data, if they so wished, would be in any way diminished by the information Defendants have collected.[18] Finally, unlike in *Facebook Tracking*, there is no evidence that Defendants have aggregated and sold Plaintiffs' browsing data to advertisers; to the contrary, it is undisputed that unmatched data is deleted after 14 days.

Under these circumstances, Plaintiffs' position boils down to an argument that every time they visit a website and a third party is informed of the visit without their knowledge, the third party has engaged in theft. Plaintiffs cite no authority for this proposition. *Cf.* JAF 91 (undisputed fact that use of the internet requires sharing of data). On this record, Plaintiffs have not shown—or even raised a fact issue—that Defendants stole their property. Defendants are entitled to summary judgment on Plaintiffs' claims for statutory larceny and conversion.

V.

Defendants' motion for summary judgment is granted, and Plaintiffs' remaining claims are dismissed on the merits with prejudice. In light of this ruling, Plaintiffs' motion for review of the magistrate judge's ruling on discovery regarding privilege issues, Dkt. No. 364, which would only impact the evidence

[18] When asked about this at the hearing, Plaintiffs' counsel stated that there was evidence of diminished value because there was a market that would pay approximately $3 per month for the kind of data collected from Plaintiffs. Even accepting this as true, Plaintiffs have not shown that Defendants' collection of their data precludes them from exploiting that market or otherwise interferes with their economic interest—i.e., that they could have sold their data for more money but for the fact that Defendants had collected it.

that could be presented at trial, is denied as moot. All future scheduling deadlines and associated obligations are vacated.

A final judgment will be entered separately.

Date: December 24, 2024

Stanley Blumenfeld, Jr.
United States District Judge